IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	W. Chou et al.
Case:	502042-A-01-US (Chou)
Serial No.:	10/668,577
Filing Date:	September 23, 2003
Group:	2143
Examiner:	Phuoc H. Nguyen
Title:	Secure Interaction Between a Mobile Client Device and an Enterprise Application in a Communication System

---

DECLARATION OF PRIOR INVENTION UNDER 37 C.F.R. §1.131

We, the undersigned, hereby declare and state as follows:

1. We are named joint inventors of the invention that is the subject of the above-referenced U.S. patent application. We have assigned our respective interests in the patent application to Avaya Technology Corp. ("Avaya").

2. The invention was conceived and actually reduced to practice at some time prior to April 19, 2002.

3. On or about April 19, 2002, an actual reduction to practice of the present invention was demonstrated to representatives of American Airlines. Relevant excerpts of an Avaya proprietary document evidencing this demonstration are attached hereto as Exhibit 1.

4. On or about April 25, 2002, inventor Wu Chou gave an internal Avaya "Show-and-Tell" presentation entitled "Dialogue System and Web Convergence – VoiceXML, HTTP and WMTIP," describing an illustrative embodiment of the present invention. An Avaya intranet web page evidencing this presentation is attached hereto as Exhibit 2. Relevant slides associated with this presentation are attached hereto as Exhibit 3.

5. On or before June 4, 2002, a paper describing the invention was prepared by the inventors. This paper is entitled "An Architecture of Wireless Web and Dialogue System Convergence for Multimodal Service Interaction Over Converged Networks." A copy of this paper is attached hereto as Exhibit 4. An electronic mail evidencing submission of this paper to the IEEE International Conference on Computer Communication and Networks (IC3N) conference on or before June 4, 2002, is attached hereto as Exhibit 5.

6. The Abstract of the paper in Exhibit 4 evidences the aforementioned actual reduction to practice of the invention: "A prototype system was implemented and performance advantages were demonstrated on several enterprise service applications." See also the Summary of the paper, Section 6, last paragraph.

7. A version of the paper in Exhibit 4 was included as pages 11-16 of U.S. Provisional Patent Application Serial No. 60/435,463, dated December 20, 2002, to which the present application claims priority.

8. All statements made herein of our own knowledge are true, and all statements made on information and belief are believed to be true.

9. We understand that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001, and may jeopardize the validity of the application or any patent issuing thereon.

Date: 4/25/2008

Wu Chou

Date: _____

Juan Jenny Li

Date: _____

Xueshan Shan

8. All statements made herein of our own knowledge are true, and all statements made on information and belief are believed to be true.

9. We understand that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001, and may jeopardize the validity of the application or any patent issuing thereon.

Date: _____ Wu Chou

Date: 04/28/2008 Juan Jenny Li

Date: _____ Xueshan Shan

8. All statements made herein of our own knowledge are true, and all statements made on information and belief are believed to be true.

9. We understand that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001, and may jeopardize the validity of the application or any patent issuing thereon.

Date: _____

_____
Wu Chou

Date: _____

_____
Juan Jenny Li

Date: April 27, 2008

Xueshan Shan Digitally signed by Xueshan Shan DN: cn=Xueshan Shan, o=Avaya, ou=Avaya Research, email=xueshanshan@hotmail.com, c=US Date: 2008.04.27 16:02:10 -07'00'

_____
Xueshan Shan

EXHIBIT 1

Demo Summaries – Avaya Labs Research

American Airlines Visit on April 19, 2002

Demo #4: Avaya WMTIP (Wireless MTIP) Enabled Dialogue System With WAP Based Multimedia Content Delivery Through Wireless Web

In this application, Avaya demonstrated a capability allowing an American Airlines passenger to contact an automated help desk by WAP-enabled cell phone (for example, from his seat in the plane after the airplane door is opened and cell phone use is allowed) and to receive customized, multimodal content addressing the passenger's needs. In the demo, the customer can get assistance on three critical needs: flight info, limo services and luggage services. The system delivers multimedia content about these services to the customer's WAP-enabled cell phone through WMTIP, a platform that is based on dialogue system and wireless web convergence. Use of this platform enables rapid development of new applications.

Specifically, in the demo applications the customer can receive information at his/her cell phone regarding their new itinerary, directions to connecting flight gate, limo driver's phone number, the direction to reach the limo driver, the luggage station and directions to luggage pick-up, etc. Information is rendered by WMTIP so that the customer will receive active rich content in the form of text, figures, maps, web page, active links, etc. The system sends a notification to customer's cell phone through the service channel. In the notification, it encodes the procedure for getting the information from WMTIP in the SI portion of WAP protocol, allowing a one-key switch to automatically get the content and eliminate the need to key in the actual web address. It provides a better user experience, high efficiency for getting the service content, and enhanced security (because the actual location of the private content is embedded in the WAP protocol and is invisible to a third party.)

The primary component in this demo was WMTIP (wireless MTIP). WMTIP includes MTIP (multimedia technology integration platform) for dialogue and content generation. MTIP is a multimodal dialogue system platform, based on hybrid-VoiceXML, which uses VoiceXML as its voice modality. A second WMTIP component is a WML content server outside the firewall that transcodes the multimedia content from MTIP for mobile devices and archives it. Finally, WMTIP has a wireless push gateway server that is connected to Sprint PCS wireless service network for service notification.

Three key takeaways Avaya would like American Airline to realize from this demo are:

1. Dialogue system and web convergence opens various new opportunities in advanced services.
2. WMTIP is Avaya Labs Research's approach for enterprise service creation and wireless web convergence.
3. The unique WAP based service delivery method in WMTIP provides active rich content to currently available 2G wireless devices and will grow in functionality with the industry's evolution to 2.5G and 3G.

EXHIBIT 2

For Insiders
Show-and-Tell Series

The weekly Show-and-Tell talk series takes place on Thursdays at 10 or 11 am. in the Auditorium.

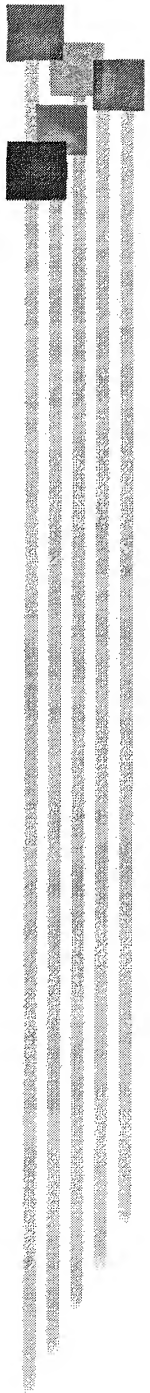
Current schedule, presentations etc. are available here.

Previous talks can be found here.

The following is a list of older talks not archived by Showbot.

Date	Speaker	Title
2002		
April 25	Wu Chou	Dialogue System and Web Convergence - VoiceXML MTIP and WMTIP

EXHIBIT 3



AVAYA labs

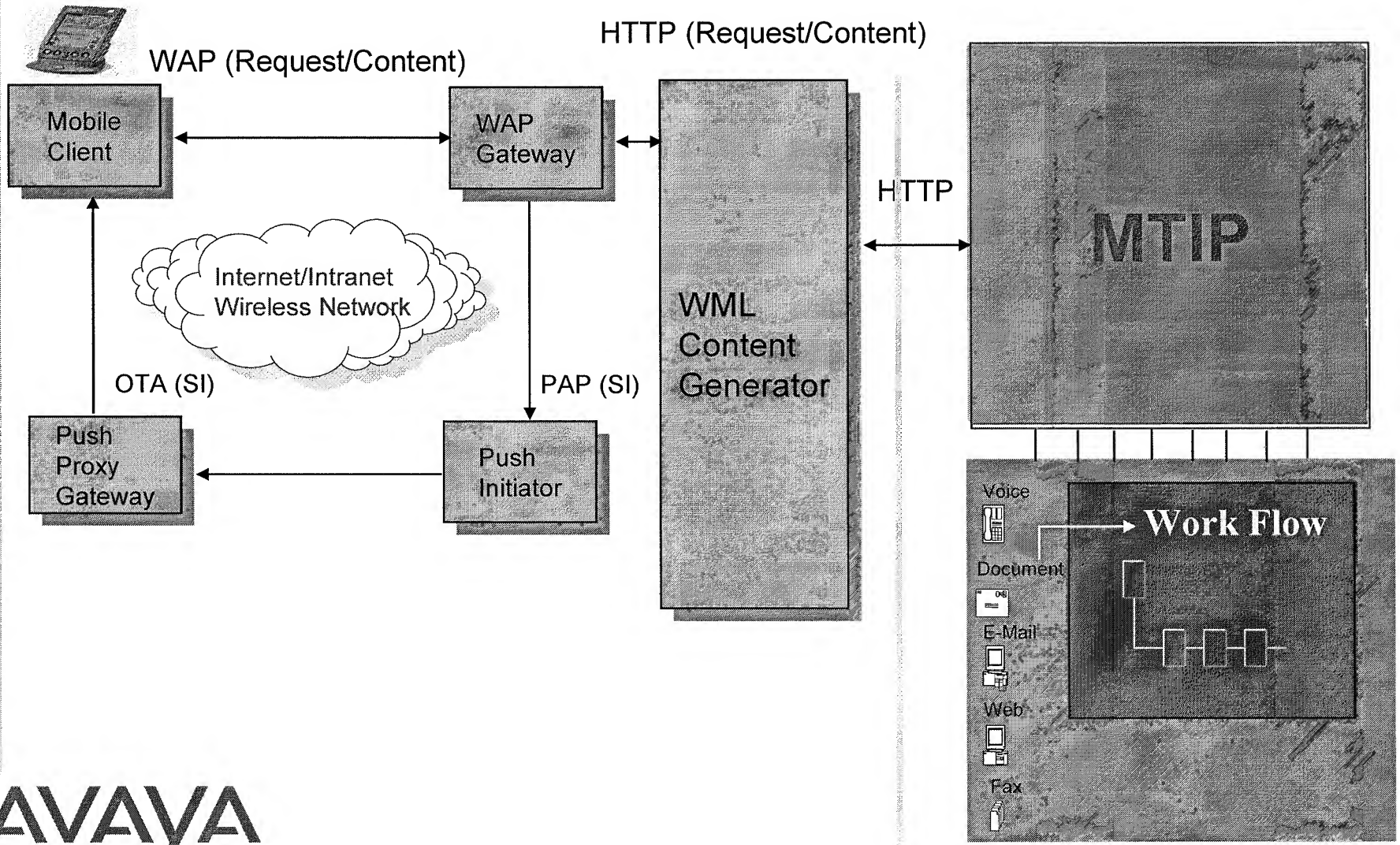
Dialogue System and Web Convergence

(VoiceXML, MTIP and WMTIP)

Wu Chou
Avaya Labs Research
Avaya Inc.
wuchou@avaya.com

Wireless Extension of MTIP Architecture

Wu Chou, Xueshan Shan and Jenny Li



AVAYA labs

WMTIP – wireless MTIP for mobile users

- **An WAP extension of MTIP**
  - Use service channel for notification and traffic channel for content delivery based on WAP 1.2.1
  - Interactive services between two channels (e.g. one key integrated switching between service and traffic channels)
  - Service initialization is embedded in notification (e.g. the link and procedures of getting the services are embedded as the SI portion of the protocol)
  - User side enhanced security: The physical link and service initiation procedures are implicit in notification and invisible to user or third party
  - Server side enhanced security: No physical connection between WML Content Generator and MTIP
  - Will be extended to leverage new broadband data services of 3G wireless

(Wu Chou, Xueshan Shan, Jenny Li)

AVAYA labs

EXHIBIT 4

An Architecture of Wireless Web and Dialogue System Convergence for Multimodal Service Interaction Over Converged Networks

Wu Chou, Xueshan Shan and J. Jenny Li
Avaya Labs Research, 233 Mt. Airy Road, Basking Ridge, NJ 07920
{wuchou, xshan, jjli}@avaya.com

Abstract

This paper presents an approach based on wireless web and dialogue system convergence for multimodal, multimedia communication services over converged networks. It uses a unique event-triggered service delivery method that separates service interaction and wireless web-based service delivery. Our approach results in an architecture of WAP-based, location-independent, wireless service monitoring, notification and service access for mobile users that can be applied over various network bearers in enterprise environment. A new wireless secure server (WSS) provides secure connections to dialogue systems. It allows one-key switching to retrieve the multimedia content. A prototype system was implemented and performance advantages were demonstrated on several enterprise service applications.

1. Introduction

The proliferation of wireless devices (cell phone, PDA, etc) has fundamentally changed the landscape of the communication services. It leads to various new challenges to provide secure service delivery, service notification and monitoring over a converged network for mobile users. In enterprise environment, the situation becomes even more acute. In order to reach mobile users, communication services have to be delivered over a heterogeneous network infrastructure involving various types of wire and wireless networks and corporate firewalls. Security for wireless access and service delivery is a serious concern. Approaches based on remote login often lead to a direct data pipe that goes through the firewall to user's mobile device. In mobile environment, such access methods have become inadequate and insecure, especially for advanced enterprise communication services with multimodal interaction and multimedia content.

In addition, unlike regular computer terminals, mobile devices are of very limited resources in terms of memory, computing power and the size of display. The communication bandwidth is also limited, and most current 2G and 2.5G cell phones do not support simultaneous data and voice communication. On the other hand, in order to enable advanced enterprise communication services, there is an increasingly critical demand for delivering active and rich multimedia content to mobile users.

In this paper, we describe approach and system architecture for secure service delivery, service monitoring and notification over converged networks for mobile users in wireless environment. This approach is based on the concept of wireless web and dialogue system convergence to overcome various issues in delivering multimodal, multimedia service interaction. The proposed approach is based on a novel integration of multimodal service interaction dialogue system and wireless web based content rendering, content delivery and embedded interactive service switching utilizing the Service Indication in WAP Push. It allows the delivery of rich and active multimedia content to the mobile users with enhanced security and improved user experience. Comparing to service delivery through SMS (short message services), the proposed approach is based on a protocol of content pulling, and therefore, it is not limited by the size and the multimedia nature of the content, which is fundamentally different from SMS. It is both forward and backward compatible since WAP is designed to operate over heterogeneous wireless environment and supported in broadband 3G wireless service standards. For non-WAP supported devices, the proposed service delivery reduces to SMS with text content.

The organization of this paper is as follows. We introduce the proposed approach and major components of the system architecture in Section 2. Section 3 is focused on new security features of Wireless Secure Server (WWS). Integration of WAP used in our approach is discussed in Section 4. Applications and advantages of the proposed approach are presented in Section 5.

2. Architecture and Approach

Traditional model for enterprise communication services often assumes that there is a direct contact channel connection between the user's end device and an

enterprise communication server. For security reason, such contact channel is most conveniently in the form of a voice channel established from a regular telephone call. Communication services are delivered by interacting with an enterprise communication server through certain type of exchanges or dialogue. The enterprise communication server is typically behind the corporate firewall and protected against any security infringing connections. In a legacy communication server, service interaction and service delivery are not separated, and all contents are delivered through the primary contact channel. In wireless mobile environment, contacts to communication services are primarily from voice channel. This imposes various constraints on the richness and the type of the services that can be supported to mobile users, leaving aside the wireless networking and device issues.

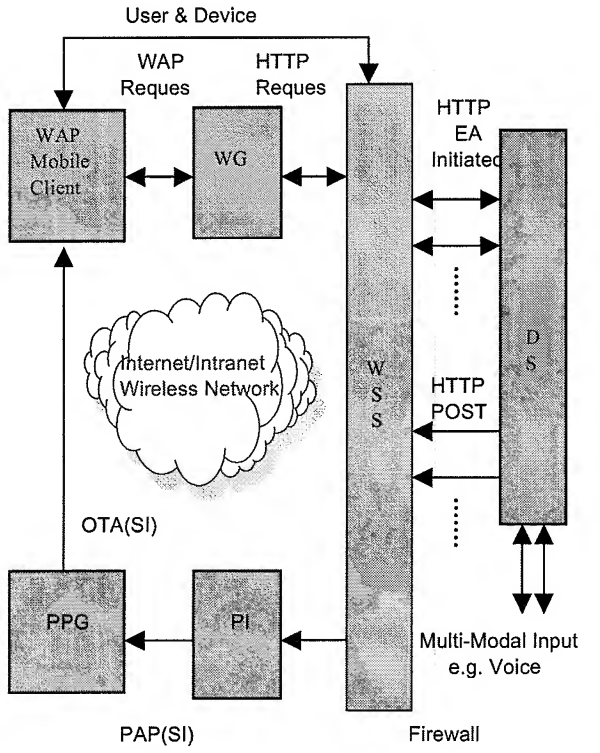


Figure 1. Architectural Flows and Protocols

In order to overcome these limitations, we adopt an event-triggered approach for wireless enabled secure service notification, multimodal service access and multimedia service content delivery. This approach is based on the concept of wireless web and dialogue system convergence. The ubiquitous of web leads to a major paradigm shift in dialogue system design and the construction of communication services. In our approach, we separate the service interaction with an enterprise communication dialogue server (DS) from the interactive event-driven service delivery. The event-driven service delivery in our approach is through a special wireless secure server (WSS) that is integrated with DS through dialogue system and web convergence. This convergence with web is carried out in two stages. First, DS is integrated with web and utilizes web and HTTP for multimedia content delivery. Secondly, WSS is integrated with both web and wireless web. It interacts with DS through web with HTTP connection, and it utilizes WAP to deliver multimedia service content to mobile client devices. Moreover, DS and WSS are active components of an enterprise communication server with wireless web as the secondary communication channel to support advanced communication services to mobile client devices.

Figure 1 illustrates the architectural system diagram of the proposed approach. In order to maintain the security, the authentication profile and secure enterprise service database are all maintained behind the corporate firewall and controlled by DS. Mobile users can access DS through a mobile device, such as a cell phone, outside the firewall. DS engages the mobile user through dialogue interaction for the purpose of user authentication and the purpose of multimedia service content generation. DS prepares the desired multimedia service content and submits it through HTTP to WSS. WSS is outside the firewall and in the public domain. It is accessible by DS from inside firewall through HTTP and by mobile client with WAP enabled mobile devices.

Figure 2. depicts the structure of WSS. A typical user registration process includes the following steps. The WAP Wireless Client can register directly through DS or register through the wireless environment with Registration Server of WSS by providing user profile manually and device profile automatically using a device profile detector on WSS. Profiles obtained through the wireless environment are stored in a FIFO User & Device Profile Queue. DS periodically pulls Register Connector and extracts pending user registration information from FIFO queue. Once extracted, the related user registration information will be deleted from the FIFO queue for the security reason.

Wireless secure information access often includes the following steps: (1) Wireless client requests for service via DS's multimodal contact channels by making a voice call or a data request. (2) DS performs authentication, identifies the service request, prepares the multimedia content, and posts it to Application Connector (AC) of

WSS via HTTP. (3) AC invokes Content Generator (CG) to generate a text notification and a dynamic URI. (4) AC invokes Push Initiator (PI) that constructs a Service Indication (SI) and sends it to PPG via Push Access Protocol (PAP). SI contains a text notification, the URI generated in step (3), and an intrusiveness level.

The service delivery in our approach is based on integrated combination of WAP Push and Pull. The procedures are described as follows: (1) PPG pushes SI to wireless client using Push Over-The-Air (OTA) protocol. (2) Wireless client displays the text notification message and the choices for URI fetching: fetch or delay. (3) WG sends request to fetch the content from Content Generator of WSS. (4) Content Generator transcodes the XML content into WML. Wireless Image Rendering Module is activated in case graphic image is involved. (5) Content Generator responds to WG with WML content via HTTP. (6) WG returns content to wireless client via WAP. Details of WAP and WAP Push integration used in our approach are given in Section 4.

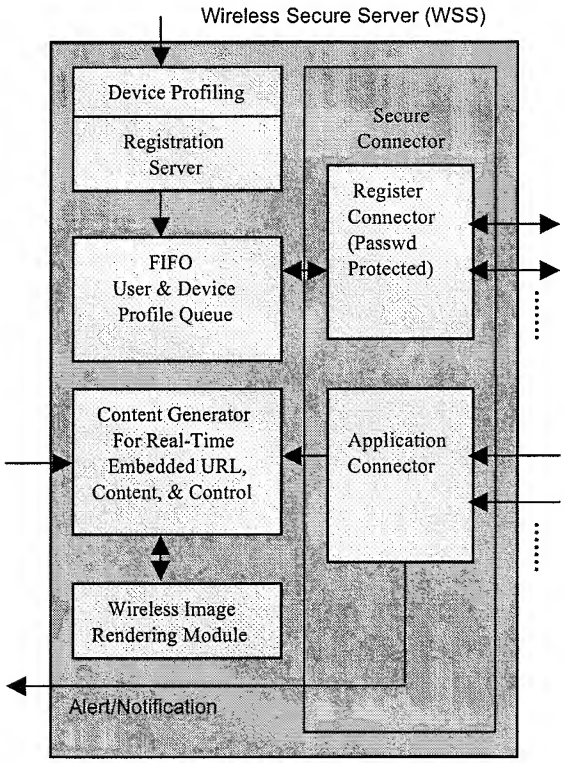


Figure 2. Details of Wireless Secure Server

3. Wireless Secure Server (WSS)

Two critical issues in designing our wireless secure server are the flexibility and security. There is a large variation in mobile network, and new devices are introduced at a random fashion. The dynamic nature of end user devices makes it critical for device dependent content transcoding, rendering and delivery. Because the server will be at public domain outside of firewalls, security is of utmost concern and has to be addressed properly in order to deliver reliable services.

The enhanced security of WSS in our approach is achieved through the following steps: 1) register password protection, 2) personalized dynamic URL and content generation, and 3) embedded URLs. In our approach, the URL content is dynamically generated as a result of the interaction with DS that happens at a separate channel and at a time before the actual content being generated and delivered to WSS. Time-stamp is used to register the particular time of the user request. Moreover, device stamp is also used to register uniquely which device is allowed to retrieve the URL content. The content with these security stamps is stored in a dynamically generated URL on WSS. In order to stop key-in peekers, the exact URL is encoded in the SI of WAP Push, which is invisible to the user and the third party. Therefore it is safe to use in a crowded public area, such as sitting in the cockpit of an airplane with people near by. In addition, the service notification and encoded procedures of accessing the content on WSS are delivered to a unique device through WAP Push based on the registered device stamp. In order to steal the content from WSS, a possible imposter has to pass the authentication process of DS, steal the registered wireless device and wireless access password to WSS and match the claimed identity. Even with all that, there is no direct data pipe through the firewall to all other corporate contents. This is because of the unique indirect content access method in our approach.

The web contextualization [6,7] is an active research area. It allows both server and client based dynamic content generation to intelligently match the device characteristics. We extended this approach for WSS because vast disparity and variations for mobile client devices. Device profile is used to address issues of device dependent transcoding and content rendering.

4. WAP and WAP Push

Wireless Application Protocol (WAP) is a result of continuous work to define an open, global specification for developing applications that operate over different wireless communication networks. It addresses mobile network characteristics and operator needs by adapting existing network technology to the special requirements of

hand-held wireless data devices and by introducing new technologies where appropriate.

To enable operators and manufacturers to meet the challenges in advanced services in the wireless market, WAP defines a set of protocols in transport, session and application layer. The essential objectives of WAP are 1) to bring Internet content and advanced data services to wireless phones and other wireless terminals; 2) to create a global wireless protocol specification that work across all wireless network technologies; 3) to enable the creation of content and applications that scale across a wide range of wireless bearer networks and device types; 4) to embrace and extend existing standards and technologies wherever appropriate.

One important part of the WAP effort is the specification of the push architecture that allows content to be sent or "pushed" by server-based applications from wired networks to WAP compliant mobile devices. Push functionality is especially relevant to real time applications that send notifications to their users, such as messaging, stock quote and traffic update alerts. Without push functionality, these types of applications would require the devices to poll application server for new information or status. In wireless environment such polling activities would constitute inefficient and wasteful use of resources of wireless networks. Moreover, entering the server's web address and page name on wireless devices is time consuming, difficult and clumsy.

4.1 WAP Architecture

The WAP architecture is defined as a layered, scalable, and extensible architecture that 1) leverages existing standards wherever possible; 2) supports as many wireless networks as possible; 3) optimizes for narrow-band bearers with high latency; 4) optimizes for efficient use of device resources; 5) provides support for secure applications and communications.

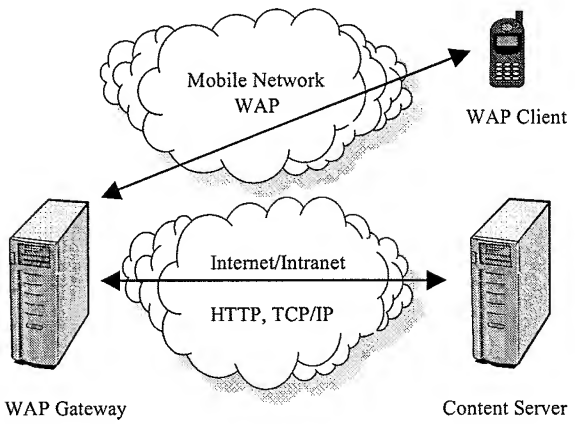


Figure 3. A Simple WAP Application Architecture

4.1.1 WAP Transaction Model

There are several steps involved in a typical WAP transaction that retrieves information from the content server: 1) User requests a URL by entering it into a WAP device; 2) The WAP device encodes the request into an encrypted, compact binary format suitable for transmission over a wireless link, and sends it to the WAP gateway; 3) The gateway examines the message, converts it into a valid HTTP-based URL request, and forwards it to the content server; 4) When the content server receives the request, it fulfills it by returning the requested document back to the gateway; 5) The gateway converts the HTTP response back into an encrypted, binary format and ships it off to the WAP device; 6) The WAP device decodes the response and displays the results on the WAP device's screen.

4.1.2 WAP Application Environment and Protocol

The WAP protocols are designed to operate over a variety of different bearer services with the capability of compensating for or tolerating these varying levels of services. The WAP standard defines 1) an application environment and 2) an application protocol.

The application protocol is a layered communication stack that consists of a session protocol, a transaction protocol, a security protocol, and a datagram protocol. The protocol stack isolates the applications from the bearer so that one application can be run regardless of the actual transport service being used.

Wireless Application Environment (WAE) consists of two things: a markup language, WML, and a programming language, WMLScript. In practice, these are realized in the microbrowser environment in a mobile terminal. WAE provides an environment that includes all the elements related to the development and execution of applications.

Wireless Session Protocol (WSP) is a session layer protocol corresponding to HTTP protocol in the wired world. It provides two types of session services: 1) a connection oriented session services over the Wireless Transaction Protocol and 2) a connectionless session services directly over the Wireless Transport layer.

Wireless Transaction Protocol (WTP) is a transport layer protocol. It provides services to accomplish reliable and

non-reliable transactions and operates over the WDP layer or over the optional security layer. WTP is optimized to adapt to the narrow bandwidth to reduce the transactions between client and server.

Wireless Transport Layer Security (WTLS) is an optional layer and is based on TLS (Transport Layer Security), which in turn is based on SSL (Secure Sockets Layer), which are Internet protocols. WTLS operates over the transport layer (WDP) to provide data protection including data integrity, privacy, authentication, and denial-of-service protection.

Wireless Datagram Protocol (WDP) is a transport layer datagram protocol corresponding to UDP protocol in the wired world. WDP shields the upper layers from the bearer services provided by the network and allows transparent transmission of data over different bearers. WDP thus makes WAP an extremely portable protocol operable on completely different mobile networks.

4.2 WAP Push Architecture and Protocol

The WAP specification defines a push architecture, which allows information to be transmitted to a device without an explicit request from the device. Figure 6 illustrates a simple WAP push architecture.

A push operation in WAP is accomplished by allowing a Push Initiator (PI) to transmit push content and delivery instructions to a Push Proxy Gateway (PPG), which then delivers the push content to the WAP client according to the delivery instructions.

The PI is typically an application running on a Web server. It communicates with PPG using Push Access Protocol (PAP). The PPG uses Push Over-The-Air (OTA) protocol to deliver the push content to the client. The PPG may notify the PI about the final outcome of a push submission and optionally handle cancellation, replacement, or client capability requests from the PI.

PAP is based on standard Internet protocols. XML is used to express the delivery instructions, and the push content can be any MIME media type. PAP can deliver three types of content. 1) Service indication (SI) which consists of asynchronous notifications. At its most basic, an SI contains a brief text message and a URI specifying a service; 2) Service Loading (SL) which allows a user agent on a client device to load and execute a service specified by a URI without user intervention; 3) Cache operation which makes it possible to invalidate content objects in the wireless client's cache.

The OTA protocol provides both connectionless and connection-oriented services. While connectionless service relies upon Wireless Session Protocol (WSP), the connection-oriented service may be provided in conjunction with both WSP (OTA-WSP) and HTTP (OTA-HTTP).

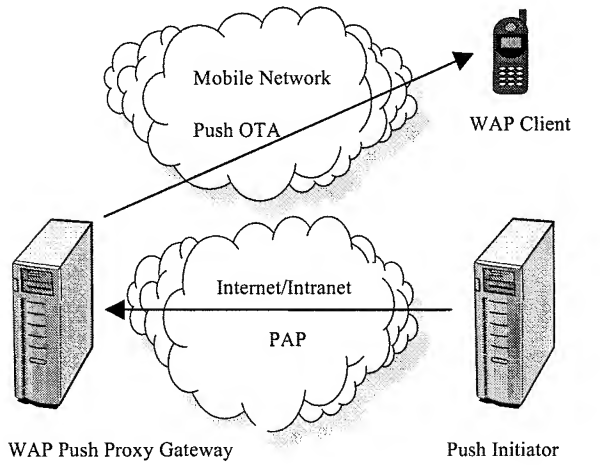


Figure 4. A Simple WAP Push Architecture

4.3 Push and Pull Based WAP Services

We adopted both push and pull mechanisms in our system design to provide WAP services for delivering event-triggered, secure notification and multimedia, active content over the mobile network. WAP push is used in sending notifications to mobile users anywhere, anytime without a data connection. WAP pull is used for detailed information access upon receiving the push content.

The integration of WAP services with the DS is achieved through a specially designed WSS. The event triggering is through the DS and relayed by the WSS. Upon receiving the event trigger from the DS the WSS first prepares the WML content and then invokes the PI to initiate a WAP push operation. When the push content, an SI in our case, reaches the mobile device via the PPG user may hit only one key to request for more detailed information. The client originated request initiates a WAP pull operation that pulls the multimedia content or a WAP application from the Content Generator of the WSS and displays it on the client device. Since active content or applications can be delivered to mobile client through pull operation our approach not only seamlessly couples WAP push and WAP pull operations and makes the transporting model transparent to users but also further facilitates the server-centric architecture, i.e. no client application running on the device, which makes the application platform device-

independent and open to any WAP enabled terminals in the market.

5. Applications and Case Study

The proposed approach is implemented as an advanced enterprise communication server. It is a wireless multimedia technology integration platform (WMTIP) to support various applications in enterprise customer relation management (CRM) services for mobile users. The DS in our implementation is based a multimedia dialogue server, MTIP, which has a distributed dialogue system architecture. The dialogue system and web convergence in MTIP is achieved through an approach based on Hybrid-VoiceXML which has VoiceXML as its voice modality [1]. WMTIP is a step further beyond MTIP with convergence of wireless web for mobile users.

Several new enterprise communication services were created through the proposed approach. One application is the direction information services for mobile users. A mobile user can call from a registered cell phone and ask for direction service to reach certain location. WMTIP engages with mobile user and delivers the multimedia service content in the forms of text, figure, maps, links, etc. following the steps and procedures described in Section 2. In particular, for direction services, a turn by turn instructions and maps are delivered, so that the mobile user does not need to memorize all turns, and instead, a hard copy of the multimedia service content will be delivered to his mobile device. These services overcome the network infrastructure and bandwidth limitation bearer in mobile environment. It is critical in the sense that these services cannot be effectively delivered by using the voice channel alone, and the ability of delivering multimedia content to mobile client devices has significantly changed the service paradigm.

The proposed approach has several unique advantages. The WAP Push-based, connectionless approach for wireless notification and URI delivery reduces the cost of airtime and power consumption and improves the user experience with one-key interactive switching. In general, enhanced security often comes with additional inconvenience for the user, but this is not the case in the proposed approach. The proposed approach allows mobile user to access the content through one-key switching, which is the best possible for 2G devices and a rare case of enhanced security with improved user experience.

6. Summary

In this paper, an approach based on wireless web and dialogue system convergence was presented and applied in enterprise environment to provide multimodal, multimedia communication services over converged networks. It uses a unique event-triggered service delivery method that separates service interaction and wireless web-based service delivery. Our approach results in an architecture of WAP-based, location-independent, wireless service monitoring, notification and service access for mobile users that can be applied over various network bearers. A new wireless secure server (WSS) was described. It provides secure connections to enterprise communication services for mobile client devices. New security features in the proposed approach were described that significantly enhance both user and server side security in mobile environment. The enhanced security in our approach comes with improved user experience. It allows one-key switching to retrieve the multimedia content. Therefore, the time consuming, error prune and inconvenient key-in process for web content is eliminated. A prototype system was implemented based on the proposed approach and performance advantages were demonstrated on several mission critical enterprise communication service applications.

REFERENCES

[1] F. Liu, A. Saad, L. Li and W. Chou, "A Distributed Multimodal Dialogue System based on Dialogue System and Web Convergence", *to appear in Proceedings, ICSLP'02*

[2] X. Shan and J. Jenny Li, "A Case Study of IP Network Monitoring Using Wireless Mobile Devices", Proc. IC3N'01, pp. 590-593

[3] K. Wang, "Implementation of Multimodal Dialog System Using Extended Markup Languages", *Proceedings of ICSLP'00*, October 2000.

[4] W3C, "Voice extensible Markup Language (VoiceXML) version 1.0", http://www.w3.org/TR/2000/NOTE-voicexml-20000505/2000

[5] G. Niklfeld, R. Finan, M. Pucher, "Architecture for Adaptive Multimodal Dialog System Based on VoiceXML",*Proceedings of EuroSpeech'01*

[6] J. Hjelm, et al., W3C Delivery Context Workshop, France, March 02.

[7] http://www.wapforum.org

EXHIBIT 5

From: Eric Wong [mailto:ewong@utdallas.edu]
Sent: Tuesday, June 04, 2002 7:16 AM
To: Wu Chou
Cc: ekpark@umkc.edu; jjli@avaya.com; xshan@avaya.com; Eric Wong
Subject: Re: IC3N

Wu:

Thank you for the submission.

Eric

Wu Chou wrote:
>
> EK, Eirc,
>
> Sorry, we are little behind the schedule due to some internal delay
> and we submit our paper to IC3N'02 with this email.
>
> Please let me know should question occur.
>
> Regards,
>
> ------Wu Chou.
>
> ----------
> Name: wmtip_cover.doc
> wmtip_cover.doc Type: WINWORD File (application/msword)
> Encoding: base64
> Download Status: Not downloaded with message
>
> ----------
>
>
> An Architecture of Wireless Web and Dialogue System Convergence for
> Multimodal Service Interaction Over Converged Networks
>
> Wu Chou, Xueshan Shan and J. Jenny Li
> Avaya Labs Research, 233 Mt. Airy Road, Basking Ridge, NJ 07920
> {wuchou, xshan, jjli}@avaya.com
>
> Abstract
>
> This paper presents an approach based on wireless web and dialogue
> system convergence for multimodal, multimedia communication services
> over converged networks. It uses a unique event-triggered service
> delivery method that separates service interaction and wireless
> web-based service delivery. Our approach results in an architecture of
> WAP-based, location-independent, wireless service monitoring,
> notification and service access for mobile users that can be applied over various network bearers in enterprise environment. A new wireless secure server (WSS) provides secure connections to dialogue systems. It allows one-key switching to retrieve the multimedia content. A prototype system was implemented and performance advantages were demonstrated on several enterprise service applications.
>
> ----------
> Name: ic3n_wmtip_submit.pdf
> ic3n_wmtip_submit.pdf Type: Acrobat (application/pdf)
> Encoding: base64
> Download Status: Not downloaded with message
